House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure protection and Security Technologies
"Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal"
June 24, 2011
Testimony of Dr. Gregory E. Shannon
Software Engineering Institute
Chief Scientist for the CERT Program

Chairman Lungren, Ranking Member Clarke, and other distinguished members of the subcommittee, thank you for the opportunity to testify, it is my pleasure to be here this morning to discuss cyber incident response.

## About CERT®

The CERT Program is part of Carnegie Mellon University's Software Engineering Institute, a federally funded research and development center, and is located on the Carnegie Mellon campus in Pittsburgh, Pennsylvania.

The CERT program (http://www.cert.org/) was charged by DARPA in 1988 to set up the first Computer Emergency Response Team (CERT) as a response to the Morris worm incident. We continue to develop and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, and restore continuity of critical services. CERT works both to mitigate cyber risks and coordinate cyber incident responses at local, national, and global levels. Over the last 23 years CERT has helped to establish over 200 CERT computer security incident response teams (CSIRTs) around the world – including the DHS US CERT. We continue to have proven success transitioning research and technology to those who can implement it on a national scale.

Dr. Greg Shannon is the Chief Scientist for the CERT Program, where he works to establish and enhance the program's research visibility, initiatives, strategies, and policies.

## Testimony

Today's operational cyber environments are complex and dynamic. User needs and environmental factors are constantly changing, which leads to unanticipated usage, reconfiguration, and continuous evolution of practices and technologies. New defects and vulnerabilities in these environments are continually being discovered, and the means to exploit these environments continues to rise. The CERT Coordination Center cataloged ~250,000 instances of malicious artifacts last month alone. From this milieu, public and private institutions respond daily to repeated attacks and also to the more serious previously un-experienced failures (but not necessarily unexpected); both demand rapid, capable and agile responses.

Incident response, as a discipline, is maturing. Over the last two decades, it has emerged from the shadows of IT and risk management, to achieve recognition as a robust and growing discipline[1]. Signs of this progress include the emergence of process models, meta-models, bodies

[1] For example, this fall, CERT and the Institute for Information Infrastructure will hold a workshop on Coordinated Private-Sector Responses to Cyber Security Incidents. This is a

of knowledge, common data representations, and auditable standards. Further development, and continued funding, will enable faster and more efficient dissemination of information to trusted partners in larger trust networks.

I applaud the current efforts of the federal government to mitigate risk to our public and private critical information infrastructures; CERT has worked tirelessly to improve cyber security in areas such as secure coding, insider threat and vulnerability analysis. But, while much is said about risk mitigation, incident response is often not as thoroughly addressed, and is critically important. Networked environments will continue to be vigorously attacked for the foreseeable future. Failure will occur and effective responses are required. Incident response is not a single action but rather a complex function that includes containment, repair, and recovery[2]. The federal government must look at incident response as strategic, just as it looks at preventative efforts. Our country needs legislation that will facilitate capable, scalable and cost-effective cyber-incident response for critical and government infrastructure. Things will fail in unexpected ways and our nation must have the capacity to respond accordingly.

I believe that the most difficult technical challenge to effective risk mitigation and incident response is selecting practices that are scientifically sound and operationally proven. The complexity of practices and regimes being proposed in legislation and elsewhere will probably have unintended and unexpected consequences. I encourage the subcommittee to use language in legislation that encourages practices that are both experimentally and operationally validated.

I believe that the most difficult policy challenge for effective government incident response is harmonizing the responsibilities, authorities, capabilities and communication across the various agencies involved. I support the current efforts in this.

In my remaining testimony I discuss three areas that we at CERT believe are key to the future of incident response.

**Information sharing**

We all realize how critical it is for stakeholders to share information, but good incident response is contingent upon sharing the right information, with the right people, at the right time. High-quality and actionable information comes from superior situational awareness only possible with robust information sharing and sufficient visibility into one's own enterprise. Currently, our technical capabilities allow us to see and respond to variant indicators, but to better detect, share and respond to incidents analysts need to be able to look past narrowly focused indicators.

---

follow on to I3P's 2009 workshop on Protecting Critical Infrastructures: The National Capital Region as a Model for Cyber Preparedness.

[2] Some contend that retaliation is part of incident response; I disagree. The response community does not consider it in scope for incident response as practiced today. Other organizations and disciplines are better suited to address this issue.

Achieving this enhanced situational awareness will require continued research on network traffic and data. The ability to detect malicious markers that are invariant, such as behavioral based indicators (e.g. insider threats) will enable a more proactive response. To facilitate innovation, richer data needs to be shared with the research community, not only incident data itself, but also data-sets that will enable an understanding of what "normal" resembles. Currently, the community does not have a clear understanding of what this data set would look like. If situational awareness is to develop beyond simple indicators, regulatory frameworks must allow access to everyday data, so that investigators can begin to recognize what data-set are important. This data sharing should start with limited access to high-fidelity datasets for researchers so that data with scientifically proven value is considered for sharing operationally. Otherwise, policymakers and experts are left to speculate what is the right data to share. To further improve the future efficiency and effectiveness of incident response, the community also needs to develop and use automated tools and techniques to analyze and correlate the vast amount of log files, artifacts, and other event information.

Moreover, compliance-driven information sharing will only lead to the bare minimum disclosure of sensitive information related to problems, concerns, and vulnerabilities. Building trusted relationships with stakeholders becomes essential to avoiding such limited information exchange and is a fundamental ingredient to a successful response. We also have to trust the people in the field and those who first respond to incidents. I applaud the effort in this legislation to support actions to do the "Right Thing™"; this is an important principle in the response community and is the basis of successful responses in many highly stressful incidents. Safe harbor measures such as Sec. 246 in the Administration's Cybersecurity Legislative Proposal work towards continued encouragement to share data; however in response scenarios it is worthwhile to consider including the actions of cyber "first responders" into good faith legislation as well.

**Forensics**

While gains have been made in the field of incident response the nature of the ever evolving cyber threat poses a huge challenge and demand for incident response expertise that has far outstripped the supply.

Computers are no longer just the targets of crime; our adversaries now use them to facilitate every aspect of their illicit activities and achieve effects at scale. Once an incident occurs federal agencies are facing several hurdles to recover the needed data in order to locate the source of the incident and contain the problem. First, computer forensic labs are constrained by a lack of resources, creating an enormous backlog rendering them unable to handle the megafold increases in the volumes of data that need to be examined for evidence. While some agencies may have the qualified examiners, and many do not, they lack the funds to properly equip them for the mission. For example, current examination methods rely heavily on processor power, but due to dramatically increased computer memory, examination stations often cannot keep up. Finally, the current state of the practice does not allow examiners to easily access varied levels of expertise in a timely or cost-effective way, frequently people are sent Temporary Duty or images are shipped to higher level units, resulting in time delays and increased costs..

To successfully respond to cyber incidents these obstacles must be overcome in a way that allows for high-quality collaborative examinations. For instance, what would happen if an adversary perpetrated an actual, severe cyber event with national consequences? Currently there is no one facility or lab that could support the volume of data these kinds of events would generate. Under current conditions, data would have to be distributed, adding to the time and complexity of conducting examinations. Agencies will need to augment scarce resources by having multiple users viewing the same data either remotely or locally, while maximizing the application of specialized computing resources, and allowing for massive, coordinated efforts. Analysts and investigators will need flexible, secure access to high-performance systems, to increase productivity and facilitate effective distributed collaboration in a scalable and cost-effective way.

**Training**

In order to rapidly handle cyber incidents the federal government needs a workforce educated and equipped to respond. However, the rapid changes and dynamic nature of cybersecurity make keeping the workforce up to date a very challenging problem. Responding to critical cyber events requires technical knowledge and skills, decision-making abilities, and effective coordination – all while moving rapidly. Moreover, a lack of preparation inhibits secondary incident handling activities, such as: evidence gathering, identifying the attacker, and reporting the incident to other affected organizations. The Federal government must have an agile and prepared workforce to deal with cyber incidents, and should to be able to train them in a cost effective and scalable manner.

The most common workforce development training solution is the traditional classroom training model. While this training model is easy to implement and is widely used, there are a number of reasons why it is not adequate for providing effective, large-scale training to a technical workforce, including time, cost and scalability. Furthermore, traditional classroom training is not optimal for rapidly changing fields such as cybersecurity.

The best way to prepare the workforce is to have them practice under realistic conditions with interactive simulations, and the ability to interface with participants across multiple locations who can work together to analyze and respond to the latest threats and attacks. Individuals need to be trained on a platform that safely mimics how the internet would respond to stress and exposes them to real-world scenarios, events, and activities that are similar to those they will encounter in their jobs.

In addition, there are two incident response domains where we see an immediate need for further training. The first is reverse engineering, to grow capacity in analyzing malware recovered from an incident. The second domain is embedded systems, which pose many unique challenges for incident response and which some experts believe will be a major cyber security problem area in the near future.

The workforce needs to not only be trained, but also educated. For example, in the case of forensics, much of the training the workforce receives is how to use tools, but when those tools are not effective no one is educated on how to manage the situation or apply critical

thinking to determine alternative approaches. What's more, to train the workforce to manage cyber incidents the federal government needs to expand the scope of computer or cyber security training to include first responder training and best practice guidance. Without proper education a first responder may unintentionally cause irrevocable damage by doing something as simple as turning off a computer. This will not only cause lost data, but can also result in severely slowing an investigation and compromise the potential prosecution of the perpetrator.

In conclusion, I thank the subcommittee again for inviting me and considering my testimony. Our nation will continue to see significant serious cyber incidents for the forseable future. CERT's mission is to help ensure that these incidents are not catastrophic and that we recover as quickly as possible. We at CERT look forward to the day when our nation's cyber resiliency is founded on the effective mitigation of cyber security risks and pervasive capabilities to respond to cyber security incidents. I see this legislation and the related modifications and efforts as an important step in the right direction.

# Additional Resources for Congress

A Framework for Modeling the Software Assurance Ecosystem: Insights from the Software Assurance Landscape Project
August 2010
TECHNICAL REPORT
CMU/SEI-2010-TR-028
ESC-TR-2010-028
http://www.sei.cmu.edu/library/abstracts/reports/10tr028.cfm

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0
April 2011
TECHNICAL REPORT
CMU/SEI-2011-TR-015
ESC-TR-2011-015
http://www.sei.cmu.edu/library/abstracts/reports/11tr015.cfm

The CERT® Approach to Cybersecurity Workforce Development
December 2010
TECHNICAL REPORT
CMU/SEI-2010-TR-045
ESC-TR-2010-110